

Appln. No.: 10/091,479
Amendment dated November 23, 2005
Reply to Office Action of July 25, 2005

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-27 (cancelled).

28. (New) A method for clustered Secure Sockets Layer (SSL) acceleration, comprising the steps of:
connecting at least two SSL relays in a cluster;
establishing a communication path between a first node and a second node via a first SSL relay of the cluster;
transferring information between the first node and the first SSL relay, the transferred information related to a communication from the first node to a second node; and
clustering state information of the communication path in response to receiving an acknowledgment from the second node confirming receipt of the communication, the clustering comprising sharing the state information between the first SSL relay and at least a second SSL relay of the relay cluster, wherein the second SSL relay is capable of taking over communications between the first and second node upon failure of the first SSL relay.

29. (New) The method according to claim 28, wherein the first node comprises a client and the second node comprises a server.

30. (New) The method according to claim 28, further comprising transferring information associated with communications between the first node and the second node to the second SSL relay transparently upon failure of the first SSL relay.

31. (New) The method according to claim 28, further comprising transmitting the communication from the first node to the second SSL relay and from the second SSL relay to the second node transparently upon failure of the first SSL relay.

Appln. No.: 10/091,479
Amendment dated November 23, 2005
Reply to Office Action of July 25, 2005

32. (New) The method according to claim 28, wherein the data communication comprises data being transferred between the first node and the second node.
33. (New) The method according to claim 32, wherein the third acknowledgment confirms receipt of the data communication by the second node.
34. (New) The method according to claim 28, further comprising sharing an SSL session cache across all of the at least two SSL relays.
35. (New) The method according to claim 28, further comprising clustering an SSL session resumption between the first node and the first SSL relay.
36. (New) The method according to claim 28, further comprising clustering cryptographic keying information across all of the at least two SSL relays.
37. (New) The method according to claim 36, further comprising clustering a key and a current Cipher Block Chaining (CBC) residue.
38. (New) The method according to claim 36, further comprising clustering a sequence number.
39. (New) The method according to claim 36, further comprising clustering a current key schedule.
40. (New) The method according to claim 36, further comprising clustering a key and an offset into a key stream.
41. (New) The method according to claim 28, further comprising clustering a cipher state.

Appln. No.: 10/091,479

Amendment dated November 23, 2005

Reply to Office Action of July 25, 2005

42. (New) The method according to claim 28, further comprising clustering data from a partial record corresponding to data from either the first or second node.

43. (New) The method according to claim 28, further comprising clustering a record size before the record is transmitted.

44. (New) A system for clustered Secure Sockets Layer (SSL) acceleration comprising:

a first node;

a second node; and

an SSL relay cluster for connecting the first node and second node comprising:

a first SSL relay configured to cluster state information in response to a first acknowledgment from the second node confirming receipt of data transmitted from the first node; and

a second SSL relay configured to transmit a second acknowledgment to the first SSL relay upon receiving the state information.

45. (New) The system according to claim 44, wherein the first node comprises a client and the second node comprises a server.

46. (New) A computer readable medium storing computer readable instructions that, when executed by a processor, performs a method comprising:

establishing a connection between a first node and a second node via a first SSL relay of an SSL relay cluster, wherein said SSL relay cluster comprises at least two interconnected SSL relays;

receiving a data communication from the first node;

transmitting the data communication to the second node;

Appln. No.: 10/091,479
Amendment dated November 23, 2005
Reply to Office Action of July 25, 2005

receiving a first acknowledgment from the second node confirming receipt of the data communication;

in response to the first acknowledgment, clustering state information of the established connection with at least a second SSL relay of the SSL relay cluster;

receiving a second acknowledgment from at least the second SSL relay in the SSL relay cluster confirming successful clustering; and

in response to the second acknowledgment, transmitting a third acknowledgment to the first node.

47. (New) The apparatus according to claim 46, wherein the second SSL relay assumes the first SSL relay's responsibilities upon failure of the first SSL relay.

48. (New) The apparatus according to claim 46, wherein the first node comprises a client and the second node comprises a server.

49. (New) An SSL relay, the SSL relay connected in a cluster of SSL relays, comprising:

a first interface for transferring information between a first node and the SSL relay;
a second interface for transferring information between a second node and the SSL relay;
a third interface for transferring state information between SSL relays in the cluster only in response to an acknowledgment from the second node confirming receipt of transferred information; and

a storage device, wherein the state information of an SSL connection between the first node and the SSL relay is shared across each SSL relay in the cluster, any of the SSL relays in the cluster capable of taking over all connections of another SSL relay in the cluster, therefore providing no interruption in the transfer of information should any of the SSL relays in the cluster fail.

Appl. No.: 10/091,479
Amendment dated November 23, 2005
Reply to Office Action of July 25, 2005

50. (New) The apparatus according to claim 49, wherein the first node is a client and the second node is a server.

51. (New) The apparatus according to claim 49, wherein the first interface and the second interface are the same.

52. (New) The apparatus according to claim 49, wherein the second interface and the third interface are the same.

53. (New) The apparatus according to claim 49, wherein the first interface and the third interface are the same.

54. (New) The apparatus according to claim 49, wherein the first interface and the second interface and the third interface are the same.